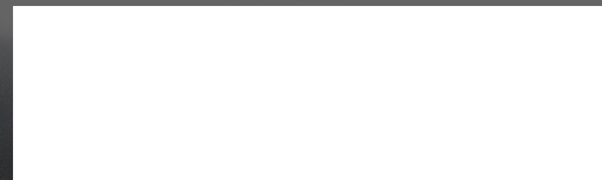


Криптография

XOR шифрование

В этом видео

1. Что такое XOR?
2. Single-byte XOR шифрование
3. Repeated-key XOR шифрование

GeekBrains

XOR (исключающее ИЛИ, сложение по модулю 2) — битовая операция, которая возвращает 0, если операнды равны и 1 в противном случае.

0 ^ 0 = 0

0 ^ 1 = 1

1 ^ 0 = 1

1 ^ 1 = 0

Fixed XOR

	W	i	k	i
	01010111	01101001	01101011	01101001
⊕	11110011	11110011	11110011	11110011
=	10100100	10011010	10011000	10011010

Fixed XOR

	W	i	k	i
	01010111	01101001	01101011	01101001
⊕	11110011	11110011	11110011	11110011
=	10100100	10011010	10011000	10011010

GeekBrains

Fixed XOR

	W	i	k	i
	01010111	01101001	01101011	01101001
⊕	11110011	11110011	11110011	11110011
=	10100100	10011010	10011000	10011010

Fixed XOR

	W	i	k	i
	01010111	01101001	01101011	01101001
⊕	11110011	11110011	11110011	11110011
=	10100100	10011010	10011000	10011010

GeekBrains

Single-byte XOR

	W	i	k	i
	01010111	01101001	01101011	01101001
⊕	11110011	11110011	11110011	11110011
=	10100100	10011010	10011000	10011010

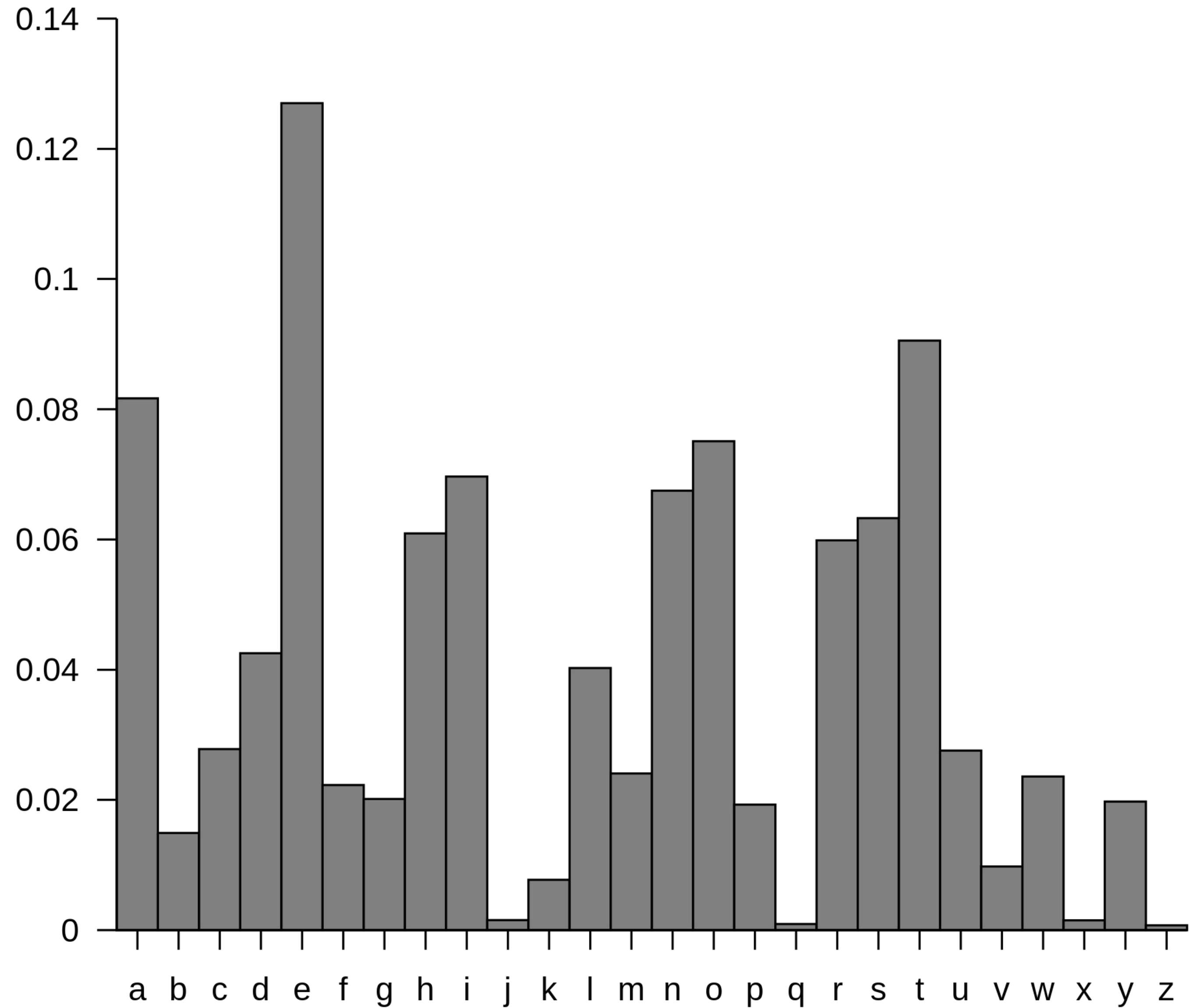
Single-byte XOR decryption

	10100100	10011010	10011000	10011010
⊕	11110011	11110011	11110011	11110011
=	01010111	01101001	01101011	01101001
	W	i	k	i

Уязвимости?

- У открытого текста неравномерное распределение символов
- Множество возможных ключей мало

Перебор ключей и частотный анализ!



Repeating-key XOR

```
  10100100 10011010 10011000 10011010
⊕ 11110011 11110011 11110011 11110011
  -----------------------------------
= 01010111 01101001 01101011 01101001

     W        i        k        i
```

Repeating-key XOR

Зашифруем открытый текст «I want to break free» на ключе «YEP».

492077616e7420746f20627265616b2066726565

XOR

7965707965707965707965707965707965707965

=

304507180b0459111f5907021c041b5903021c00

GeekBrains

Как взломать такой шифр?

Найти длину ключа

Восстановить ключ с помощью модифицированного частотного анализа

Расстояние Хэмминга — количество отличающихся бит. Например, расстояние Хэмминга для 01001100 и 10011101 равно 4.

Найти длину ключа

Взять два (четыре, шесть, …) блоков шифротекста и найти расстояние Хемминга между ними.

Поделить на длину блока (нормализовать).

GeekBrains

304507180b0459111f5907021c041b5903021c00

304507 ^ 180b04

=

796570 ^ 492077 ^ 796570 ^ 616e74

=

284e03

Найти ключ

Разобьем шифротекст на блоки длины ключа и транспонируем («повернем») их особым образом.

304507180b0459111f5907021c041b5903021c00

\/

301859591c591c

450b1107040300

07041f021b02

\/

Частотный анализ single-byte XOR

GeekBrains

Итоги

1. Научились применять XOR
2. Узнали как работает single-byte XOR шифрование
3. Узнали принцип работы и слабости Repeated-key XOR шифрования